IN THE UNITED STATES DISTRICT COURT SOUTHERN DISTRICT OF TEXAS HOUSTON DIVISION

CELL Film Holdings, LLC,	§ §
Plaintiff,	§ §
v.	§ Case No. <u>4:16-cv-02544</u>
Does 1–15, anonymous BitTorrent users participating in file-sharing swarm identified by hash ending in 2EA8,	\$ \$ Jury \$ \$
Defendants.	§ §

PLAINTIFF CELL FILM HOLDINGS, LLC'S *EX PARTE*MOTION TO TAKE PRE-26(F) CONFERENCE DISCOVERY
OF THIRD-PARTY INTERNET SERVICE PROVIDER

COURT PROCEDURE 6.A.4 NOTE

Due to the ex parte nature of this motion and the fact that there will be no opposition as all Doe defendants cannot be identified if and until the Court rules favorably, the Court may wish to consider this motion prior to the typical submission date.

TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION	2
II. NATURE AND STAGE OF THE PROCEEDING	5
III. ISSUE TO BE RULED UPON AND STANDARD OF REVIEW	6
IV. A SHORT SUMMARY OF THE ARGUMENT	7
V. ARGUMENT	8
A. Plaintiff Has Made a Concrete Showing of a Prima Facie Claim of Actionable Harm	9
B. Plaintiff Has Proposed Clear and Specific Discovery Requests	10
C. Plaintiff Has No Alternative Means to Obtain the Information	12
D. Plaintiff Needs the Subpoenaed Information to Advance the Claim	13
E. Plaintiff's Interest in Obtaining the Subscribers' True Identities Outweighs Subscribers' Interest in Remaining Anonymous	14
VI. CONCLUSION	

TABLE OF AUTHORITIES

FEDERAL CASES Arista Records, LLC v. Doe 3, 604 F.3d 110 (2d Cir. 2010)7 Bell Atl. Corp. v. Twombly, 127 S. Ct. 1955 (2007)......9 Columbia Ins. Co. v. Seescandy.Com, Garrett v. Comcast Comms., Inc., General Universal Sys., Inc. v. Lee, 379 F. 3d 131 (5th Cir. 2004)......9 In re Verizon Internet Servs., Inc., 257 F. Supp. 2d 244 (D.D.C. 2003)......14 Patrick Collins, Inc. v. John Doe 1, 945 F. Supp. 2d 367 (E.D.N.Y. 2013)......9 Owest Comms. Int'l, Inc. v. Worldquest Networks, Inc., Recording Indus. v. Verizon Internet, 351 F. 3d 1229 (D.D.C. 2003)......12 Sony Music Entm't Inc. v. Does 1–40. St. Louis Grp., Inc. v. Metals & Additives Corp., Inc., 275 F.R.D. 236 (S.D. Tex. 2011)6 W. Coast Prods., Inc. v. Does 1-351, No. 4:12-cv-504, 2012 WL 2577551 (S.D. Tex. July 3, 2012)......... 5, 11, 15 Well Go USA, Inc. v. Unknown Participants,

STATUTES

17 U.S.C. § 512(h)	12
47 U.S.C. § 551(1)(a)	8, 15
47 U.S.C. § 551(c)(1)(B)	13

Case 4:16-cv-02544 Document 5 Filed in TXSD on 08/22/16 Page 4 of 22

	47 U.S.C. § 551(c)(2)	13
	47 U.S.C. § 551(d)	13
<u>R</u> u	<u>ULES</u>	
	FED. R. CIV. P. 26(d)(1)	6, 7
	FED. R. CIV. P. 26(f)	6
	FED. R. CIV. P. 45	

Plaintiff, CELL Film Holdings, LLC ("CFH"), hereby moves this Court *ex parte* requesting an order granting limited pre-26(f) conference discovery. Specifically, plaintiff seeks to issue a subpoena to an internet service provider ("ISP") Comcast Communications Management, L.L.C. ("Comcast") pursuant to FED. R. CIV. P. 45 for information sufficient to identify each defendant (currently listed as Does 1–15), including name, current and permanent address, telephone number, and e-mail address.

Each Doe defendant has been observed as using torrent networks to distribute an infringing copy of plaintiff's copyrighted motion picture. However, plaintiff has only been able to identify each defendant by his or her internet protocol ("IP") address shown in Exhibit 2 to the Complaint and attached here as Exhibit 1. It is therefore necessary for plaintiff to obtain the identity of the subscriber corresponding to the IP address.

ISPs routinely provide the identity of a subscriber corresponding to a particular IP address under the Digital Millennium Copyright Act ("DMCA"), and in fact, the ISPs often provide a special facsimile number for facilitating service of this type of subpoena when issued by law enforcement officials. A sample subpoena is attached as Exhibit 2.

Plaintiff will use any obtained information solely for the purpose of protecting Plaintiff's rights as set forth in its Complaint.

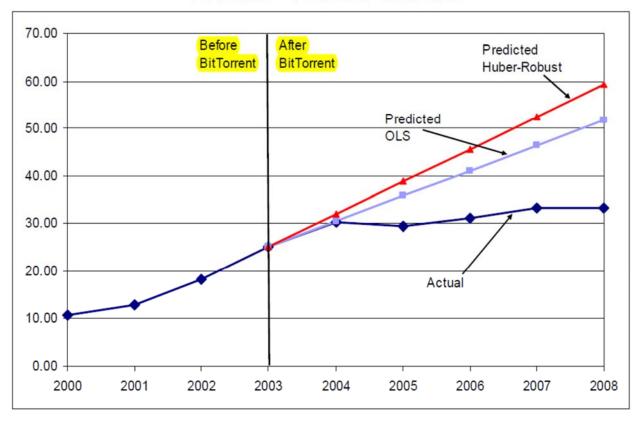
I. INTRODUCTION

A 2015 U.S. Executive Report noted that unauthorized distribution of motion picture recordings via the Internet is doing tremendous damage to film producers, distributers, and copyright holders.¹ This economic harm is illustrated in the graphs below from a University of Texas research paper, showing the precipitous decline in video and DVD sales coinciding with the rise of BitTorrent file sharing.²

Ex. 3, Ambassador Froman, 2015 Special 301 Report, Executive Office of the President of the United States (finding unauthorized recordings of first-run motion pictures result in economic harm not only in the market where the film was originally shown, but in other markets as well and that governments must not create "a domestic environment that offers a safe haven for piracy on the Internet"), available at https://ustr.gov/sites/default/files/2015-Special-301-Report-FINAL.pdf.

² Ex. 4, Zentner, Measuring the Impact of File Sharing on the Movie Industry: An Empirical Analysis Using a Panel of Countries, at 2 & 23, University of Texas at Dallas (Mar. 22, 2010), available at http://ssrn.com/abstract=1792615 ("Our findings, in short, indicate that the unauthorized downloading of movies decreases video sales by a substantial amount.").





The Department of Justice is addressing this plague of BitTorrent infringement. In July 2016, the DOJ announced the arrest of the mastermind behind the most visited illegal file-sharing website, *Kickass Torrents*.³ A criminal complaint filed in Chicago charges him with conspiracy to commit money laundering and criminal copyright infringement. The DOJ estimates this one website was responsible for

³ Ex. 5, U.S. Authorities Charge Owner of Most-Visited Illegal File-Sharing Website with Copyright Infringement, Dept. of Justice Press Release (July 20, 2016), available at https://www.justice.gov/opa/pr/us-authorities-charge-owner-most-visited-illegal-file-sharing-website-copyright-infringement.

unlawfully distributing well over \$1 billion of copyrighted materials and was the 69th most frequently visited website on the internet.

And Texas Representative Lamar Smith further notes with respect to such BitTorrent internet havens like these that:

Because the U.S. produces the most intellectual property, our nation has the most to lose if we fail to address the problem of rogue sites. According to estimates, IP theft costs the U.S. economy more than \$100 billion annually and results in the loss of thousands of American jobs.⁴

Unfortunately, while the DOJ has arrested the owner of one site, there are countless other similar websites, operating from remote corners of the world, that continue to facilitate illegal distribution of motion pictures, music and ebooks, using BitTorrent software. Downloaders can even consult "top ten pirated movie lists" to steer them to the hottest titles.

Locally, the University of Houston announced it will begin blocking BitTorrent peer-to-peer data traffic on the University of Houston Wi-Fi network "to limit illegal downloading of copyrighted material and comply with state and federal laws."⁵

⁴ Ex. 6, Smith: Law Needed to Control Cyber Piracy, Austin American-Statesman (Nov. 28, 2011), available at http://www.statesman.com/news/news/opinion/smith-law-needed-to-control-cyber-piracy/nRhYk/.

⁵ Ex. 7, University of Houston IT Notice, available at http://rationalrights.com/?p=502.

CFH is a victim of such piracy. Plaintiff owns the copyright for the movie Cell ("Motion Picture"), a mainstream motion picture with well-known actors. [Dkt. 1 ¶¶ 30–31 & Ex. 1.] Although the movie was released in the U.S. only recently, already CFH has identified 15 IP addresses located in the Southern District of Texas as participating in a group copying and distributing an unauthorized copy of CFH's Motion Picture, without license, via an online peer-to-peer ("P2P") torrent network system. [Dkt. 1 ¶¶ 45–51 & Ex. 2.]

II. NATURE AND STAGE OF THE PROCEEDING

In an attempt to stop this unauthorized distribution of the Motion Picture, plaintiff filed a Complaint alleging copyright infringement. [Dkt. 1.] For each defendant, CFH was only able to identify the defendant infringer by the IP address the infringer used to commit the infringement. [Id.] As explained in the Complaint, only the ISP knows which subscribers were associated with the IP addresses at the relevant times. As such, CFH named pseudonymous "Doe" defendants associated with the IP addresses, as is convention. See, e.g., W. Coast Prods., Inc. v. Does 1–351, No. 4:12-cv-504, 2012 WL 2577551 (S.D. Tex. July 3, 2012) (Doc. 30) (Atlas, J.) (App. at 3).

Now, CFH is filing this ex parte motion to serve a subpoena on the

ISP so that plaintiff may obtain the identities of the account holders corresponding to the IP addresses at the times plaintiff observed the infringement. Having the ability to issue a subpoena on the relevant ISP will allow plaintiff to contact the subscriber and, if necessary, amend the Complaint and serve the same.

III. ISSUE TO BE RULED UPON AND STANDARD OF REVIEW

Plaintiff seeks an order permitting limited, pre-Rule 26(f), discovery from a third-party for the purpose of identifying the Doe defendants. FED. R. CIV. P. 26(d)(1) provides that "[a] party may not seek discovery from any source before the parties have conferred as required by Rule 26(f)" unless the Court orders otherwise, and this Court has adopted a "good cause" standard to determine whether to permit such expedited discovery. *St. Louis Grp., Inc. v. Metals & Additives Corp., Inc.*, 275 F.R.D. 236, 240 (S.D. Tex. 2011).

When considering if "good cause" exists for motions to identify the accounts associated with IP addresses, this Court considers: "(1) a concrete showing of a prima facie claim of actionable harm by the plaintiff; (2) specificity of the discovery request; (3) the absence of alternative means to obtain the subpoenaed information; (4) a central need for the subpoenaed information to advance the claim; and (5) the user's expectation of

privacy." Well Go USA, Inc. v. Unknown Participants, No. 4:12-cv-963 (S.D. Tex. Sept. 25, 2012) (Ellison, J.) (citing Arista Records, LLC v. Doe 3, 604 F.3d 110, 114 (2d Cir. 2010)) (App. at 8–9).

IV. A SHORT SUMMARY OF THE ARGUMENT

CFH has set forth in detail a *prima facie* case that its copyright has been, and is being, infringed by people whom plaintiff can now only identify by the IP addresses they used in committing the infringement. Plaintiff has filed suit and wishes to use discovery requested in this motion to identify the true identities of these infringers. But the default Federal Rules—written for the typical case where the true identity of the defendant is known to plaintiff—specify that discovery can only be initiated after the plaintiff and defendant's conference. *See* 26(d)(1). Yet, to confer, plaintiff needs the sought after discovery to know with whom to confer.

To break this "Catch 22," CFH proposes obtaining specific, limited, information regarding the identity of the subscribers who were responsible for these IP addresses at the times of observed infringement from their ISP—the only entity that can identify those persons. And in an attempt to minimize any burden on the ISP, plaintiff is requesting minimal information it needs to advance the litigation—information ISPs regularly provide to copyright owners in the DMCA context. Because the ISPs only

keep the needed data for a limited time, without the relief sought, plaintiff's opportunity to identify the defendants may soon be lost forever.

Finally, while defendants may be hoping to maintain the anonymity the Internet affords to infringe with impunity, Does 1–15 should not expect it. Semi-anonymous peoples from around the world have been using BitTorrent technology to illegally copy the Motion Picture from computers connected to the BitTorrent community through the subscriber's internet account. The subscriber should not be heard to complain when the owner of the copyright asks the ISP to provide information to identify the subscriber. Indeed, by statute, ISPs initially and regularly notify subscribers that their information is subject to disclosure via court order. 47 U.S.C. § 551(1)(a); see also Ex. 8, Comcast Privacy Notice. And defendants' willful violation of copyright law is just the type of activity that would invite such a court order.

In short, in order for plaintiff to advance its claim and seek relief from the harm done by defendants—people who should have no expectation of privacy for their illegal activity—the Court should allow the narrowly tailored discovery to the sole source of the information, the ISP.

V. ARGUMENT

The following subsections establish why the good cause factors all

favor allowing plaintiff's requested early third-party discovery.

A. Plaintiff Has Made a Concrete Showing of a Prima Facie Claim of Actionable Harm

"To establish a prima facie case of copyright infringement, a copyright owner must prove (1) ownership of a valid copyright, and (2) copying by the defendant of constituent elements of the work that are original." *General Universal Sys., Inc. v. Lee*, 379 F. 3d 131, 141 (5th Cir. 2004) (internal quotes, citations, and modifications removed). At the pleading stage, a plaintiff simply must provide "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 127 S. Ct. 1955, 1974 (2007). And "plausible" simply means having an appearance of truth or reason, a lower threshold than a "reasonable likelihood" standard. *See Patrick Collins, Inc. v. John Doe 1*, 945 F. Supp. 2d 367, 376 (E.D.N.Y. 2013).

As to the first element, copyright interest, plaintiff filed a copyright certificate for Cell [Dkt. 1 Ex. 1] which "is prima facie evidence both that a copyright is valid and that the registrant owns the copyright." *General Universal Sys.*, 379 F. 3d at 141.

As to the second element, evidence of copying, CFH has engaged the services of Maverickeye UG ("Maverickeye"), a company that specializes in monitoring and detecting the illegal distribution of material, such as

motion pictures, via P2P distribution systems. [Ex. 10, Wyde Decl. ¶2.] Maverickeye's software detected and logged the IP addresses distributing an unauthorized copy of plaintiff's Motion Picture at the dates and times shown in the exhibit attached to the complaint. [Dkt. 1 Ex. 2; Ex. 10, Wyde Decl. ¶3.]

Further, through geolocation services, including the Maverickeye software's geolocation feature, it was confirmed that all IP addresses were located in the Southern District of Texas. [Ex. 10, Wyde Decl. ¶4.]

B. Plaintiff Has Proposed Clear and Specific Discovery Requests

The relevant inquiry is whether "[p]laintiffs' discovery request is . . . sufficiently specific to establish a reasonable likelihood that the discovery request would lead to identifying information that would make possible service upon particular defendants who could be sued in federal court." *See Sony Music Entm't Inc.*, v. Does 1-40, 326 F. Supp. 2d. 556, 566 (S.D.N.Y. 2004) (citing *Columbia Ins. Co. v. Seescandy.Com*, 185 F.R.D. 573, 578 (N.D. Cal. 1999)).

Here, plaintiff's discovery request satisfies this requirement by asking for the subscriber information that corresponds to an IP address at a specific date and time where plaintiff's agents observed infringing activity. It is reasonable to suspect that this subscriber conducted the alleged activity, but even if the IP addresses cannot pinpoint a person responsible

for a particular file download this Court has found that:

Nevertheless, it is reasonable to use an IP address as a starting point to obtain identifying information about a Doe Defendant who, through digital forensic means, has been tied to the torrent swarm in issue. The identifying information allows Plaintiff to make a good faith investigation into whether a particular individual has a reliable factual connection to the IP address associated with the swarm.

W. Coast Prods., No. 4:12-cv-504 (App. at 5). At a minimum, obtaining the subscriber information will allow plaintiff's counsel to assess whether pursuit of claims against each subscriber is in fact feasible once the individual associated with the IP address has been identified. As discussed in the following subsection, plaintiff has no other way to do this.

The subpoena is narrowly tailored to get the required information, and as this is the type of data normally kept in the regular course of business, the request should impose minimal burden on the ISP. Indeed, for almost 20 years, in other situations, Congress has provided copyright holders the ability to serve subpoenas for this type of information regarding works stored on an ISP server without having to file a lawsuit or motion a court.

⁶ The situation is analogous to capturing the license plate of a car that committed a violation. The driver is likely the owner, but, if not, the owner is the person most liable to know who was driving his or her car at the time of the incident.

See DMCA, Pub. L. No. 105–304, 112 Stat. 2860 (Oct. 28, 1998) (codified at 17 U.S.C. § 512(h)). As such, ISPs are already well equipped to handle these routine requests.

C. Plaintiff Has No Alternative Means to Obtain the Information

Although CFH's agents are able to observe defendants' infringing activity through forensic software, plaintiff is unable to access defendants' identifying information, other than the IP addresses they used to commit the infringement. [Ex. 10, Wyde Decl. ¶6.] Nor is plaintiff able to upload a file onto defendants' computers or otherwise communicate with defendants in a manner that would provide notice of suit. Hence, plaintiff must contact the ISP the defendants used when committing the infringement to learn the subscriber's information in order to communicate with them and/or amend the Complaint to use defendants' true names.

But plaintiff cannot simply ask the ISP for the requested information.

Under the Cable Communications Policy Act of 1984, as amended:

However, this provision does not appear to contemplate the situation where an ISP is acting as a conduit for P2P file sharing, which is understandable because at the time of the DCMA, P2P software like BitTorrent was "not even a glimmer in anyone's eye." *Recording Indus. v. Verizon Internet*, 351 F. 3d 1229, 1238 (D.D.C. 2003) (citation omitted). It appears this issue has not been decided in this district or circuit. *See, e.g., Garrett v. Comcast Comms., Inc.*, No. 3:04-cv-693, n.1 (N.D. Tex. July 23, 2004) [Dkt. 15] ("This Court is not bound to follow the precedent of *RIAA v. Verizon.*"). (App. at 2.)

[A] cable operator shall not disclose personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned and shall take such actions as are necessary to prevent unauthorized access to such information by a person other than the subscriber or cable operator.

47 U.S.C. § 551(c)(1)(B). As such, the ISP requires a subpoena to release the name and address of subscribers. *Id.* § 551(c)(2).

Moreover, time is of the essence. Per statute, "[a] cable operator shall destroy personally identifiable information if the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access to such information." *Id.* § 551(e). Therefore, if the subpoenas are not issued quickly, the subscriber information may be permanently lost. *See Qwest Commc'ns Int'l, Inc. v. Worldquest Networks, Inc.*, 213 F.R.D. 418, 419 (D. Colo. 2003) (recognizing expedited discovery may be appropriate if "physical evidence may be consumed or destroyed with the passage of time").

D. Plaintiff Needs the Subpoenaed Information to Advance the Claim

The information that plaintiff seeks to subpoen from the ISPs is necessary to advance its claims against the infringers. Because the ISPs are not named defendants, this is not a case of whether to provide immediate access to the requested discovery rather than postponing its ultimate

production until the normal course of discovery. Rather, the information requested is a prerequisite needed so that: (1) the defendants may be notified so that they may answer; (2) the Court may have a complete and informed Case Management Conference with defendants present; and (3) litigation, including normal discovery, can commence. The subscriber information simply must be identified before this suit can progress further.

E. Plaintiff's Interest in Obtaining the Subscribers' True Identities Outweighs Subscribers' Interest in Remaining Anonymous

Plaintiff has a strong and legitimate interest in protecting its copyrighted content, and has established it cannot advance its claims without the ability to identify the individuals responsible for downloading and distributing plaintiff's copyrighted movie. In contrast, the subscribers cannot make a sound claim to retaining their anonymity.

First, the subscribers have little expectation of privacy because they voluntarily allowed their internet accounts to be used to distribute copyrighted information to others through P2P file sharing. *In re Verizon Internet Servs., Inc.*, 257 F. Supp. 2d 244, 267 (D.D.C. 2003), *rev'd on other grounds, Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Servs., Inc.*, 351 F.3d 1229 (D.C. Cir. 2003) ("[I]f an individual subscriber opens his computer to permit others, through peer-to-peer file-sharing, to download materials from that computer, it is hard to understand just what

privacy expectation he or she has after essentially opening the computer to the world.").

Second, the subscribers are on notice that Comcast prohibits its internet service for any use that "infringe[s] the rights of others," and that their information may be disclosed "with or without the subscriber's consent, and with or without notice, in compliance with the terms of valid legal process such as a subpoena."

Indeed, the Cable Act requires ISPs to notify customers of the possibility of this disclosure at the time of entering into an agreement to provide service and at least once a year thereafter. § 551(1)(a).

Third, "to the extent that anonymity is used to mask copyright infringement or to facilitate such infringement by others, the First Amendment is no protection." *W. Coast Prods.*, No. 4:12-cv-504 (App. at 5) (citing *Sony Music Entm't Inc. v. Does 1–40*, 326 F. Supp. 2d 556, 567 (S.D.N.Y. 2004) ("[D]efendants' First Amendment right to remain

Ex. 9, Comcast's Terms of Use ("[P]rohibited uses and activities include ... using the Service, Customer Equipment, or the Comcast Equipment, either individually or in combination with one another, to: ... upload, post, publish, transmit, reproduce, create derivative works of, or distribute in any way information, software or other material obtained through the Service or otherwise that is protected by copyright or other proprietary right, without obtaining any required permission of the owner.").

⁹ Ex. 8, Comcast's Privacy Notice.

anonymous must give way to plaintiffs' right to use the judicial process to pursue what appear to be meritorious copyright infringement claims.")).

Fourth, it is standard procedure for ISPs to provide subscribers with sufficient time to make an appearance to object to the disclosure of the subscriber's information, request a protective order, or request other relief. Therefore, if the subscribers wish to argue that their information should not be publicly disclosed, they will have an opportunity to be heard.

VI. CONCLUSION

As shown above, every factor the Court considers when determining if good cause exists militates in favor of allowing the pre-26(f) conference discovery. Therefore, CFH respectfully requests the Court to grant its motion. A proposed Order is attached.

Dated: August 22, 2016 Respectfully submitted,

s/Joshua S. Wyde/

Joshua S. Wyde, Attorney-in-Charge

Tex. State Bar No. 24060858

S.D. Tex. Bar No. 873284

THE LAW OFFICE OF JOSHUA S WYDE

3740 Greenbriar St. #980609

Houston, TX 77098-0609

Tel: 713.482.1916

Fax: 713.466.6563

jwyde@wydelegal.com

Gary J. Fischman

Tex. State Bar No. 787469

S.D. Tex. Bar No. 17126

FISCHMAN LAW PLLC 710 N. Post Oak Rd. Suite 105 Houston, TX 77024–3808 Tel: 713.900.4924 fischman@fischmaniplaw.com

Attorneys for Plaintiff, CELL Film Holdings, LLC

CERTIFICATE OF SERVICE PER LR5

As the true identities of the defendants are unknown at this time, service is not possible and this motion is being filed *ex parte*.

Dated: August 22, 2016 _____ s/Joshua S. Wyde/ Joshua S. Wyde

CERTIFICATE OF CONFERENCE PER COURT PROCEEDURE 6.A.2

Plaintiffs do not know the identity of the defendants, and, as such, are unable to confer.

Dated: August 22, 2016 s/Joshua S. Wyde/
Joshua S. Wyde